DATE(S) ISSUED:
09/17/2012

SUBJECT:
Vulnerability in Novell GroupWise Internet Agent Could Allow Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Novell GroupWise Internet Agent which could allow remote code execution. Novell GroupWise is a collaborative software product, which includes email, calendars, instant messaging and document management. The GroupWise Internet Agent (GWIA) is a server component that provides communication to other email systems and conversion of email messages to GroupWise format.

Successful exploitation could allow an attacker to gain the same privileges as the affected application. An attacker could then install programs; view, change, or delete data; or create new accounts. Unsuccessful exploitation attempts may result in a denial of service.

Please note that exploit code is publicly available for this vulnerability.

SYSTEMS AFFECTED:
> Novell GroupWise Internet Agent
> Novell GroupWise 8.0x through 8.0.2 HP3
> Novell GroupWise 2012

RISK:
Government:
> Large and medium government entities: **High**
> Small government entities: **High**

Businesses:
> Large and medium business entities: **High**
> Small business entities: **High**

Home users: N/A

DESCRIPTION:
Novell has confirmed the existence of an integer-overflow vulnerability in Novell GroupWise Internet Agent that may allow remote code execution. The vulnerability occurs due to the way the Internet Agent processes the "Content-Length" header value, specifically, the issue occurs when the value is set to -1.

Successful exploitation could allow an attacker to gain the same privileges as the affected application. An attacker could then install programs; view, change, or delete data; or create new accounts. Unsuccessful exploitation attempts may result in a denial of service.

Please note that exploit code is publicly available for this vulnerability.

Novell has released updates for GroupWise version 8 only. A fix will be released in late September 2012 for GroupWise 2012.

RECOMMENDATIONS:
The following actions should be taken:
> For GroupWise 8 users, apply the appropriate updates provided by Novell to vulnerable systems immediately after appropriate testing
> For GroupWise 2012 users, apply appropriate updates provided by Novell to vulnerable systems as soon as they become available in late September.
> Consider disabling the GWIA WebConsole in GroupWise 2012 or blocking access to default port 9850 until a patch is released and applied.

REFERENCES:
Novell:
http://www.novell.com/support/kb/doc.php?id=7010769

SecurityFocus:
http://www.securityfocus.com/bid/55551/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0271